

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-056326

(43)Date of publication of application : 20.02.2002

(51)Int.Cl.

G06F 17/60
G11B 27/00

(21)Application number : 2000-241576

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 09.08.2000

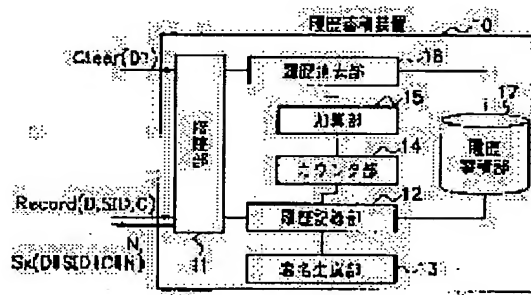
(72)Inventor : FUJIMURA TAKASHI
TERADA MASAYUKI
NISHIHARA TAKUO

(54) HISTORY ACCUMULATION DEVICE, VERIFICATION DEVICE, AND ELECTRONIC RIGHT DISTRIBUTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To reliably check the number of utilized times of an electronic right utilizable a fixed number of times on an off-line basis and to safely erase unnecessary data.

SOLUTION: Out of the history data including an effective period, a service ID, and the number of accumulation times stored in a history accumulating section 17, only the time-expired history data can be erased by a history erasing section 16. The data D0 when the history erasing section 16 has previously erased the history data is stored in a merely incremental counter section 14. When a history recording section 12 receives a history record request including the effective period D and the service ID via a connecting section 11, it compares D with the data D0 of the counter section 14 and terminates the operation if D is smaller, thereby prevents such fraud that the same history data are recorded after the history data are erased, with the data set forward, and prevents the history accumulating section 17 from becoming full with data.



LEGAL STATUS

[Date of request for examination] 07.01.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3723429

[Date of registration] 22.09.2005

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-56326

(P2002-56326A)

(43) 公開日 平成14年2月20日 (2002.2.20)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 17/60	4 1 0	G 0 6 F 17/60	4 1 0 A 5 B 0 4 9
	1 4 2		1 4 2 5 B 0 5 5
	4 3 2		4 3 2 A 5 D 1 1 0
	5 1 0		5 1 0
G 1 1 B 27/00		G 1 1 B 27/00	A
審査請求 未請求 請求項の数 8 O L (全 11 頁)			

(21) 出願番号 特願2000-241576(P2000-241576)

(22) 出願日 平成12年8月9日 (2000.8.9)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 藤村 考

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 寺田 雅之

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100069981

弁理士 吉田 精孝

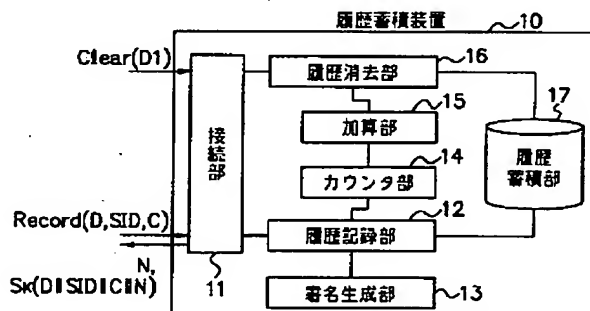
最終頁に続く

(54) 【発明の名称】 履歴蓄積装置、検証装置および電子権利流通システム

(57) 【要約】

【課題】 一定の回数利用可能な電子権利の利用回数をオフラインで確実にチェックでき、かつ不要なデータを安全に消去すること。

【解決手段】 履歴蓄積部17に蓄積された有効期限、サービスID及び累積回数を含む履歴データのうち、有効期限が切れた履歴データのみ履歴消去部16による消去を可能とするとともに、インクリメントしかできないカウンタ部14に履歴消去部16が以前に履歴データを消去した日付D0を格納させておき、有効期限D及びサービスIDを含む履歴記録要求を接続部11を介して履歴記録部12が受けた際、Dとカウンタ部14の日付D0とを比較し、Dの方が小さい場合は例外終了させることにより、日付を進めて履歴データを消去した後、同じ履歴データを記録するような不正を防止するとともに履歴蓄積部17がデータで一杯になるのを防止する。



【特許請求の範囲】

【請求項 1】 サービス有効期限とサービス識別子と累積サービス回数を含む履歴データのリストを蓄積する履歴蓄積部と、第 1 の日付データを格納するカウンタ部とを有し、サービス有効期限とサービス識別子を含む履歴記録要求を受信する手段と、前記サービス有効期限が前記第 1 の日付データより大きいか比較する手段と、大きい場合に前記サービス有効期限とサービス識別子を含む履歴データを前記履歴蓄積部に格納する手段と、前記履歴記録要求の処理結果を送信する手段と、第 2 の日付データを含む履歴消去要求を受信する手段と、第 2 の日付データが第 1 の日付データよりも大きいか比較する手段と、大きい場合に第 2 の日付データをカウンタ部に格納する手段と、第 2 の日付データより小さい有効期限を有する履歴データを履歴蓄積部から削除する手段と、前記履歴消去要求の処理結果を送信する手段とを備えたことを特徴とする履歴蓄積装置。

【請求項 2】 請求項 1 に記載の履歴蓄積装置において、前記履歴記録要求はチャレンジを含み、履歴蓄積装置の鍵により前記サービス有効期限と前記サービス識別子とチャレンジを含むデータに対してデジタル署名を行う署名生成手段を備え、前記履歴記録要求の処理結果は、前記デジタル署名を含むことを特徴とする履歴蓄積装置。

【請求項 3】 履歴蓄積装置と接続する接続手段と、履歴蓄積装置にサービス有効期限とサービス識別子を含む履歴記録要求を送信する手段と、前記履歴記録要求の処理結果を履歴蓄積装置から受信する手段とを備えたことを特徴とする検証装置。

【請求項 4】 請求項 3 に記載の検証装置において、チャレンジを生成する手段と、履歴蓄積装置にサービス有効期限とサービス識別子とチャレンジを含む履歴記録要求を送信する手段と、前記履歴記録要求の処理結果に含まれるデジタル署名を検証する署名検証手段とを備えたことを特徴とする検証装置。

【請求項 5】 前記請求項 3 又は 4 に記載の検証装置において、日付データを含む履歴消去要求を送信する手段を備えたことを特徴とする検証装置。

【請求項 6】 発行装置と電子財布装置と改札装置とから構成される電子権利流通システムにおいて、発行装置は請求項 3 乃至 5 いずれかに記載の検証装置を含み、電子財布装置は請求項 1 又は 2 に記載の履歴蓄積装置を含み、

また、発行装置は履歴記録要求を電子財布装置に送信する手段を有し、

また、電子財布装置は前記履歴記録要求の処理結果を発行装置に送信する手段を有し、

また、発行装置は前記処理結果を検証し制約条件を充足しているか検証する手段と、制約条件を充足している時にのみ電子権利を発行する手段とを有することを特徴とする電子権利流通システム。

【請求項 7】 請求項 6 に記載の電子権利流通システムにおいて、

電子財布装置はさらに請求項 3 乃至 5 いずれかに記載の検証装置を含み、

また、電子財布装置は履歴記録要求を譲渡先の電子財布装置に送信する手段と、履歴記録要求の処理結果を譲渡元の電子財布装置に送信する手段と、前記処理結果を検証し制約条件を充足しているか検証する手段と、制約条件を充足している時にのみ電子権利を譲渡する手段とを有することを特徴とする電子権利流通システム。

【請求項 8】 発行装置と電子財布装置と改札装置とから構成される電子権利流通システムにおいて、改札装置は請求項 3 乃至 5 いずれかに記載の検証装置を含み、

電子財布装置は請求項 1 又は 2 に記載の履歴蓄積装置を含み、

また、改札装置は履歴記録要求を電子財布装置に送信する手段を有し、

また、電子財布装置は前記履歴記録要求の処理結果を改札装置に送信する手段を有し、

また、改札装置は前記処理結果を検証し制約条件を充足しているか検証する手段と、制約条件を充足している時にのみ電子権利を改札する手段とを有することを特徴とする電子権利流通システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、利用者に提供するサービスで回数制限が設けられているもの、例えば優待券利用、バーゲン品購入、試供品引換、人気コンサートチケット購入、アンケート回答、人気投票等を IC カード等の耐タンパ装置を用いて制限回数を超えて不正にサービスを受けることを防止するための方法とその装置に関するものである。

【0002】

【従来の技術】 近年、紙で流通しているチケットやクーポンを電子化して、ネットワーク上で流通させる電子権利流通システムが多数提案されている。例えば、特願 2000-038875 号のように、IC カード等の耐タンパ装置を使用して、偽造、改ざん、二重使用を防止し、安全に流通させるための方法や、特開 2000-123095 号のように、多様な種別のチケットやクーポンを共通の装置で流通させるための方法に関するもの等

がある。

【0003】しかし、これら従来の二重使用を防止する電子権利流通システムは、一旦発行された一枚の電子権利の二重使用を防止可能にするものであって、バーゲン品の購入あるいは試供品の受け取りを一人一つ限り等に制限することや、人気投票において同一人物が複数回投票券を取得して二重に投票することを防止する方法を提供するものではない。

【0004】同じ利用者によって同じ種類の権利が制限回数以上行使されることを防止する第一の方法としては、電子権利の発行システムにおいて電子権利の発行履歴をデータベースに保存し、発行時にこのデータベースを参照して同一の利用者に対して制限回数を超過して電子権利を発行しないように制御するという方法がある。

【0005】しかし、この方法でチェックが可能になるのは発行時だけであるため、譲渡が許されている電子権利の場合には効果がない。例えば、紙のチケットと同様に多くのアルバイトを雇って電子チケットの買い占めを行い、別の利用者に高く販売する、いわゆるダブ行為は防止できない。

【0006】また、同様の方法として、電子権利の改札履歴をデータベースに保存し、発行時ではなく改札時にこのデータベースを参照して同一の利用者に対して制限回数を超過して電子権利を改札しないように制御するという方法もある。

【0007】しかし、この方法でも、発行時のチェックと同様に譲渡が許されている電子権利の場合には効果がない。また、ネットワークに接続してデータベースにアクセスすることが必要となるため、高速な改札が要求される応用では、適用することが困難な場合があった。

【0008】そこで、これらの問題を解決するための第二の方法としては、これらの各権利の行使あるいはサービスの提供の履歴を利用者自身が保有するＩＣカード等の耐タンパ装置に記録し、サービスを提供する際に利用者にＩＣカードの提示を求め、提示されたＩＣカードの履歴を調べることににより既に制限回数を超過していないかを確認する方法が考えられる。

【0009】この方法ではオフライン環境であっても高速に確認できるが、使用履歴が単調に増加していくため、ＩＣカードのように記憶容量が小さい装置では、記憶領域がすぐに一杯になってしまうという問題があった。

【0010】

【発明が解決しようとする課題】本発明は、以上の問題点を解決するためのものであり、例えば試供品引換、優待券利用、バーゲン品購入、人気コンサートチケット購入、アンケート回答、人気投票等のように、一利用者が一定期間内に受けられるサービスに回数制限が設けられる場合に、この制限を超過しているかどうかをオフラインで確実にチェックする方法と装置を提供することを目的

としており、特に、上記第二の方法によって利用者自身が保持するＩＣカード等の耐タンパ装置にサービス提供の履歴を記録する方法において、不要な履歴を安全に削除する機能を提供することにより必要となる記憶容量を削減することにある。

【0011】

【課題を解決するための手段】前記目的を達成するため、本発明の請求項１では、サービス有効期限とサービス識別子と累積サービス回数を含む履歴データのリストを蓄積する履歴蓄積部と、第１の日付データを格納するカウンタ部とを有し、サービス有効期限とサービス識別子を含む履歴記録要求を受信する手段と、前記サービス有効期限が前記第１の日付データより大きいと比較する手段と、大きい場合に前記サービス有効期限とサービス識別子を含む履歴データを前記履歴蓄積部に格納する手段と、前記履歴記録要求の処理結果を送信する手段と、第２の日付データを含む履歴消去要求を受信する手段と、第２の日付データが第１の日付データよりも大きいと比較する手段と、大きい場合に第２の日付データをカウンタ部に格納する手段と、第２の日付データより小さい有効期限を有する履歴データを履歴蓄積部から削除する手段と、前記履歴消去要求の処理結果を送信する手段とを備えたことを特徴とする履歴蓄積装置を提案する。

【0012】前記構成によれば、サービス有効期限が第１の日付データより大きい場合のみ履歴データが記録または更新されて履歴記録要求の処理結果が返却され、サービス提供の可否の判断が可能になり、また、第２の日付データが第１の日付データよりも大きい場合のみ第２の日付データより小さい有効期限を有する履歴データが削除されるため、サービスの回数制限をオフラインで確実にチェックできるとともに不要な履歴データのみを安全に削除できる。

【0013】また、本発明の請求項２では、請求項１に記載の履歴蓄積装置において、前記履歴記録要求はチャレンジを含み、履歴蓄積装置の鍵により前記サービス有効期限と前記サービス識別子とチャレンジを含むデータに対してデジタル署名を行う署名生成手段を備え、前記履歴記録要求の処理結果は、前記デジタル署名を含むことを特徴とする履歴蓄積装置を提案する。

【0014】前記構成によれば、前述した履歴蓄積装置がデジタル署名を付与された履歴記録要求の処理結果を生成でき、前記処理結果の不正な改ざん防止が可能になる。

【0015】また、本発明の請求項３では、履歴蓄積装置と接続する接続手段と、履歴蓄積装置にサービス有効期限とサービス識別子を含む履歴記録要求を送信する手段と、前記履歴記録要求の処理結果を履歴蓄積装置から受信する手段とを備えたことを特徴とする検証装置を提案する。

【0016】前記構成によれば、前述した履歴蓄積装置

の履歴データを取得でき、サービス提供の可否を確実にチェックできる。

【0017】また、本発明の請求項4では、請求項3に記載の検証装置において、チャレンジを生成する手段と、履歴蓄積装置にサービス有効期限とサービス識別子とチャレンジを含む履歴記録要求を送信する手段と、前記履歴記録要求の処理結果に含まれるデジタル署名を検証する署名検証手段とを備えたことを特徴とする検証装置を提案する。

【0018】前記構成によれば、前述した履歴蓄積装置が生成した履歴記録要求の処理結果に付与されたデジタル署名を検証でき、前記処理結果の不正な改ざん防止が可能になる。

【0019】また、本発明の請求項5では、前記請求項3又は4に記載の検証装置において、日付データを含む履歴消去要求を送信する手段を備えたことを特徴とする検証装置を提案する。

【0020】前記構成によれば、前述した履歴蓄積装置中の不要な履歴データのみを安全に削除できる。

【0021】また、本発明の請求項6では、発行装置と電子財布装置と改札装置とから構成される電子権利流通システムにおいて、発行装置は請求項3乃至5いずれかに記載の検証装置を含み、電子財布装置は請求項1又は2に記載の履歴蓄積装置を含み、また、発行装置は履歴記録要求を電子財布装置に送信する手段を有し、また、電子財布装置は前記履歴記録要求の処理結果を発行装置に送信する手段を有し、また、発行装置は前記処理結果を検証し制約条件を充足しているか検証する手段と、制約条件を充足している時にのみ電子権利を発行する手段とを有することを特徴とする電子権利流通システムを提案する。

【0022】前記構成によれば、サービスの利用回数に制限があるような電子権利を安全に発行させることが可能になる。

【0023】また、本発明の請求項7では、請求項6に記載の電子権利流通システムにおいて、電子財布装置はさらに請求項3乃至5いずれかに記載の検証装置を含み、また、電子財布装置は履歴記録要求を譲渡先の電子財布装置に送信する手段と、履歴記録要求の処理結果を譲渡元の電子財布装置に送信する手段と、前記処理結果を検証し制約条件を充足しているか検証する手段と、制約条件を充足している時にのみ電子権利を譲渡する手段とを有することを特徴とする電子権利流通システムを提案する。

【0024】前記構成によれば、サービスの利用回数に制限があるような電子権利を安全に譲渡させることが可能になる。

【0025】また、本発明の請求項8では、発行装置と電子財布装置と改札装置とから構成される電子権利流通システムにおいて、改札装置は請求項3乃至5いずれか

に記載の検証装置を含み、電子財布装置は請求項1又は2に記載の履歴蓄積装置を含み、また、改札装置は履歴記録要求を電子財布装置に送信する手段を有し、また、電子財布装置は前記履歴記録要求の処理結果を改札装置に送信する手段を有し、また、改札装置は前記処理結果を検証し制約条件を充足しているか検証する手段と、制約条件を充足している時にのみ電子権利を改札する手段とを有することを特徴とする電子権利流通システムを提案する。

【0026】前記構成によれば、サービスの利用回数に制限があるような電子権利を安全に改札させることが可能になる。

【0027】

【発明の実施の形態】〔実施の形態1〕図1は、利用者が行った行為の履歴を格納する、本発明の履歴蓄積装置の実施の形態の一例を示す構成図である。

【0028】本発明では、この履歴蓄積装置は行政機関やクレジットカード発行機関等によって各利用者に一個ずつ配布されるものとする。同一の利用者に対して複数個配布しないようにするためには、免許証、保険証、指紋等を提示させ、既に配布していないかをチェックする等の方法がある。

【0029】図1に示すように、履歴蓄積装置10は、接続部11、履歴記録部12、署名生成部13、カウンタ部14、加算部15、履歴消去部16および履歴蓄積部17から構成される。

【0030】接続部11は、後で述べる検証装置とデータの授受を行う部分である。履歴記録部12は、接続部11から受信した履歴記録要求に基づき履歴を記録する部分である。署名生成部13は、この履歴蓄積装置が保有する秘密鍵によりデジタル署名を生成する部分である。

【0031】カウンタ部14は、履歴消去日付を格納する部分であり、後で詳しく述べるように履歴消去要求によって指定された日付データが格納される。加算部15は、カウンタ部14の値を増加させる部分である。履歴消去部16は、接続部11から受信した履歴消去要求に基づき履歴を消去する部分である。

【0032】履歴蓄積部17は、履歴データを蓄積する部分であり、蓄積される履歴データの一例を図2に示す。図2に示すように、履歴蓄積部17には、＜有効期限、サービスID、累積回数＞の3つの組を含む履歴データの集合が格納される。

【0033】サービスID(SID)は、サービス提供者が利用者に対して提供するサービスを識別するための識別子であり、例えば特定の試供品の引換、特定のバーゲン品の購入、特定の人気投票等を識別するための識別子であり、サービス提供者によって付与される。

【0034】また、人気コンサートチケットの購入枚数の制限という例においても制限を与える範囲、対象によ

って様々なSIDの付与方法がある。例えば、ある特定のアーティストがある特定の年に開催するイベントに対して全てに同じSIDを付与しても良いし、ある特定のアーティストの特定の日時に開催されるイベントに対して同じSIDを付与しても良い。さらには、全てのイベントに対して異なるSIDを付与しても良い。

【0035】このようにSIDは基本的にサービス提供者の意図によって自由に設定することができる。但し、異なる事業者間で同じSIDが使用されることを防止するため、本実施の形態では、サービス提供者の秘密鍵とサービス提供者が特定のサービスに対して付与した識別子との連結に対するハッシュ値を利用するものとする。

【0036】なお、別の実施の形態としては、IETFで標準化されているURI (Internet Resource Identifier) の形式で付与し、各事業者が管理しているドメインネームをそのURIに含めることで、同じSIDが使用されるのを防いでも良い。

【0037】有効期限はSIDによって指定されるサービスが有効な期限であり、本実施の形態ではSID毎に一意の有効期限が与えられるものとする。例えば、バーゲン品の購入の場合にはその購入期限、人気投票の場合には投票期限がそれに相当する。

【0038】累積回数はSIDによって指定されるサービスを過去何回受けたかを記録する領域であり、サービスを受ける度に1増加する。

【0039】履歴蓄積装置10は、基本的に履歴記録要求と履歴消去要求の2つの要求を受け付ける。これらの要求は、接続部11によって検証装置から受信し、それぞれ履歴記録部12および履歴消去部16で処理される。履歴記録要求を受け取った場合の履歴記録部12の処理フローを図3に示す。履歴消去要求を受け取った場合の履歴消去部16の処理フローを図4に示す。

【0040】履歴記録部12は次のようなフローで履歴記録要求を処理する(図3)。

【0041】(1) 接続部11から有効期限D、サービスID(SID)、チャレンジCを含む履歴記録要求Record(D, SID, C)を受信する(s1)。なお、チャレンジCは検証装置によって生成される乱数等である。

【0042】(2) Dと、カウンタ部14に格納されている履歴消去日付とどちらが大きい(どちらが新しい)か比較し(s2)、Dの方が小さい(古い)場合には、例外終了する。

【0043】(3) 履歴蓄積部17から同じD, SIDを有する履歴データを検索する(s3)。

【0044】(4) 上記(2)により既に履歴データ<D, SID, N>が存在した場合(s4)には、累積回数NをN+1に加算して履歴データを更新する(s5)。

【0045】(5) 上記(2)により履歴データが存在しなかった場合には、新しい履歴データとして<D, SID, 1>を履歴蓄積部17に記録する(s6)。

【0046】(6) 上記(5)において履歴蓄積部17の容量不足のため、履歴が記録できなかった場合(s7)には、履歴域不足例外を発生し終了する。

【0047】(7) DとSIDとNとCの連結を署名生成部13へ送り、履歴蓄積装置10が保有する秘密鍵Kにより、署名 $S_K(D \parallel SID \parallel C \parallel N)$ を生成する(s8) (但し、履歴データが存在しなかった場合(上記(4))は $N=0$ とする)。

【0048】(8) 接続部11により要求元に対してNと $S_K(D \parallel SID \parallel C \parallel N)$ を送信(返却)する(s9)。

【0049】なお、過去のサービス提供回数を調べるだけで履歴を追加しない履歴参照要求を備えても良いが、本実施の形態では、履歴記録要求の処理結果で過去のサービス提供回数を返すことで、その機能を包含するようにした。しかし、上記履歴参照要求は上記(4)、(5)、(6)のステップを省略することで容易に実現できる。

【0050】上記の履歴記録要求を受信し上記のように処理すると、履歴データが単調に増加し、ICカード等の記憶容量が小さい装置では、すぐに記憶領域が一杯になってしまうという問題がある。そこで本発明では、図4に示すフローで有効期限を過ぎた履歴を削除する機能を持たせ、電子媒体の永続的な取引を可能にする。

【0051】履歴消去部16は、次のようなフローで履歴消去要求を処理する(図4)。

【0052】(1) 接続部11から履歴消去日付D1を含む履歴消去要求Clear(D1)を受信する(s11)。履歴消去日付は過去に履歴消去要求によって指定された履歴消去日付より後であり、かつ現在日付より以前である値を指定されるものとする。例えば、検証装置等により現在日付より一日乃至一週間程度前の日付を指定すれば良い。

【0053】(2) カウンタ部14に記録されている以前に与えられた履歴消去日時D0を取得してD1と比較し、D1がD0以下の時は例外を発生させる(s12)。

【0054】(3) $X = D1 - D0$ を計算し、加算部15でカウンタ部14にXを加算する(s13)。これによってカウンタ部14に記録される履歴消去日時はD1となる。カウンタ部14に対する演算はこのように加算しかなく、減算は存在しない一方向性のものとする。カウンタをこのように増加のみ設定可能とする方法としては、例えば、特許第1884135号等に記載された専用回路を使う方法やROMに書き込まれたソフトウェアによって実現する方法等がある。

【0055】(4) 履歴蓄積部17に格納された履歴デ

ータの中で、上記D1より以前の履歴データを検索し、消去する(s14)。

【0056】(5) 接続部11により要求元に対して正常終了を送信する(s15)。

【0057】上記のステップにより、悪意のある利用者が上記(1)のステップで将来の日付を履歴消去日付として与えて履歴消去要求を行い取引履歴を消去すると、カウンタ部14に記録されている履歴消去日時が将来の日付となるため、再度、同じ履歴を格納しようとしても、図3に示した履歴記録要求のフローのステップ

(2)により例外終了するため、不正があったことを検出することができる。また、カウンタ部14に記録されている履歴消去日時を過去の日付に戻そうとしても、前述したようにカウンタ部14の値は減算することができないので、このような不正を防止できる。

【0058】図5は、サービス提供者がサービスを提供する前に利用者から提示された履歴蓄積装置を検証し、サービスを提供して良いか判断するための、本発明の検証装置の実施の形態の一例を示す構成図である。

【0059】図5に示すように、検証装置20は、乱数生成部21、サービスID記録部22、有効期限記録部23、検証制御部24、署名検証部25、履歴消去制御部26、タイマ部27、接続部28および表示部29から構成される。

【0060】乱数生成部21は、履歴蓄積装置10を認証するためのチャレンジを生成するための部分である。サービスID記録部22および有効期限記録部23は、それぞれ検証装置20が検証したいサービスに対するサービスIDおよび有効期限を記録する部分である。検証制御部24は、検証処理を制御する部分である。

【0061】署名検証部25は、履歴蓄積装置10から送信された署名データを検証し履歴蓄積装置10を認証する部分である。履歴消去制御部26は、履歴消去要求を生成し送信する部分である。タイマ部27は、現在時刻を生成する部分である。接続部28は、履歴蓄積装置10と接続する部分である。表示部29は、検証者および利用者に対してサービスを提供できるかどうかを表示する部分である。

【0062】図6に検証装置による検証処理フローを示す。検証制御部24は次のフローで履歴蓄積装置10に記録された履歴を調べ、サービスを提供して良いか検証する。

【0063】(1) 履歴蓄積装置10を検証装置20に接続する(s21)。履歴蓄積装置10が接触型ICカードで実現されている場合には、カードが挿入された契機、非接触型ICカードで実現されている場合には、カードが近づけられたことを感知した契機で接続される。

【0064】(2) 乱数生成部21により乱数Cを生成する(s22)。

【0065】(3) サービスID記録部22および有効

期限記録部23からSIDおよびDを取得し、履歴記録要求Record(D, SID, C)を接続部11により履歴蓄積装置10に送信する(s23)。別の実施の形態では表示装置を使って利用者に提供できるいくつかのサービスを表示し、利用者あるいは検証者によって選択されたサービスに対応するSID, Dを取得しても良い。

【0066】(4) 接続部11から前記要求の結果として、過去のサービス提供回数Nと履歴蓄積装置10による署名SK(D || SID || C || N)を受信する(s24)。また、履歴域不足例外が通知された場合は、それを表示部29で表示する。

【0067】(5) 署名検証部25により、上記(4)によって取得した署名データが正しいかを検証する(s25)。検証するためには、履歴蓄積装置10の検証鍵、即ち公開鍵方式の場合には公開鍵、共通鍵方式の場合には共通鍵が必要であるが、本実施の形態では、これらは予め署名検証部25が保持しているものとする。

【0068】(6) 表示部29に過去のサービス提供回数Nを表示する(s26)。検証者は、制限回数以下であればサービス提供を許可する。例えば、試供品引換の場合には、過去に引き渡されていないこと(N=0)、バーゲン品購入の場合にはその購入制限数以下である時に、サービスを提供する。

【0069】図7に、履歴域不足例外等のエラーにより履歴が記録できなかった場合に、履歴消去要求を行う履歴消去制御部26の処理フローを示す。

【0070】(1) 表示部29から履歴消去の指示が入力される(s31)。

【0071】(2) タイマ部27から現在日付を取得する(s32)。

【0072】(3) 現在日付より一日乃至一週間程度前の日付を履歴消去日時D1として指定し、利用者に履歴を消去することを通知(表示)する(s33)。

【0073】(4) 利用者からOKの指示が出ると、接続部28により履歴蓄積装置10に対して履歴消去要求Clear(D1)を送信する(s34)。

【0074】(5) 接続部28から結果を受信し、表示部29に表示する(s35)。

【0075】[実施の形態2] 上記実施の形態は、予め履歴蓄積装置を会員カード等の形態で配布しておくことにより、会員全員に一律等しいサービスを提供するような場合、例えば会員全員に対して記念品を1個配布する場合では、会員にメール等で周知するだけで、引換券等の権利を予め発行することなく、会員カード一枚に一個だけを安全に配布できるという従来にはない特徴がある。

【0076】実施の形態2では、この機能と従来から存在する電子権利の流通システムとを組み合わせ、会員全員ではなく、特定の電子権利の発行あるいは行使に伴

う制限回数を制御する例を示す。典型例としては人気コンサートチケットの購入を一人限定枚に限る場合等である。

【0077】図8は、前述した履歴蓄積装置と検証装置を利用した、本発明の電子権利流通システムの実施の形態の一例を示す構成図である。

【0078】図8に示すように、本システムは、発行装置100、電子権利格納装置200、改札装置300およびネットワーク装置400から構成される。

【0079】発行装置100は電子権利を発行する機関、電子権利格納装置200は利用者、改札装置300は電子権利を改札する機関によって保有されるものとし、それぞれ発行者毎、利用者毎、改札者毎に複数個存在して良い。

【0080】発行装置100は、電子権利生成部101、電子権利発行部102、通信部103および検証装置104から構成される。

【0081】電子権利格納装置200は、通信部201、格納制御部202、行使制御部203、電子権利格納部204、履歴蓄積装置205および検証装置206から構成される。なお、本装置は電子財布とも称する。

【0082】改札装置300は、電子権利改札部301、通信部302および検証装置303から構成される。

【0083】なお、履歴蓄積装置205および検証装置104、206、303は、実施の形態1で述べたものと同じである。

【0084】ネットワーク装置400は、インターネットや電話網等のパブリックネットワークあるいはLANや専用線等を利用したプライベートネットワークであり、発行装置100、電子権利格納装置200および改札装置300は、本装置を介して相互に通信可能とする。

【0085】電子権利は、上記装置間で次に述べる発行、譲渡、消費、提示の4種類のトランザクションによって流通する。

【0086】発行トランザクション：電子権利を生成し、その電子権利の所有権を利用者に与えるトランザクションである。本実施の形態では、発行装置100が電子権利を生成し、これを利用者が保有する電子権利格納装置200の電子権利格納部204に格納することによって実現するものとする。

【0087】譲渡トランザクション：電子権利の所有権をある利用者から別の利用者に移転させるトランザクションである。本実施の形態では、譲渡側の利用者が保有する電子権利格納装置200の電子権利格納部204に格納されている電子権利を取り出し削除し、譲受側の利用者が保有する電子権利格納装置200の電子権利格納部204に格納することによって実現するものとする。

【0088】消費トランザクション：電子権利の所有権

を無効にするトランザクションである。本実施の形態では、利用者が保有する電子権利格納装置200の電子権利格納部204に格納されている電子権利を取り出し削除し、改札装置300に削除したことを通知することによって実現するものとする。

【0089】なお、発行、譲渡、消費のトランザクションの過程で、不正に複製が作られ、電子権利が多重使用されることを防止する方法については本発明の対象とするところではなく、既に提案されている電子権利の多重使用防止方法を本発明と組み合わせて実施することが容易であるので、詳細は省略する。

【0090】電子権利の多重使用防止方法については、例えば、特開平11-213068号、特開2000-123095号等に記載されているように、流通対象の電子権利に譲渡リストを添付し、二重使用が発覚した場合に不正者を特定できるようにすることで不正を抑止する方法、特願2000-038875号等に記載されているようなICカード等の耐タンパ装置に原本情報（トークン）を保管し、原本情報を安全に流通可能にさせるプロトコルを提供することにより不正な複製を防止する方法、特願平11-310090号等に記載されているようなネットワーク上に各電子権利に対する所有者認証情報を管理することで正当な所有者を認証する方法等、多数の方法が提案されている。

【0091】図9は電子権利格納部204に格納される電子権利のデータ構造の一例を示す説明図である。本図に示すように、一つの電子権利は、サービス（権利）ID、有効期限、回数制限およびその他の電子権利の内容が定義された権利情報の4つのデータ域を含んでいる。電子権利の取引制限を与えるために、実施の形態1で示したサービスID、有効期限が電子権利に設定されている。

【0092】回数制限は、上記有効期限内に取引が許される回数の上限値が指定される。本実施の形態では、発行あるいは譲渡トランザクションによって新たな電子権利が電子権利格納装置200に格納されることを取引とみなす。即ち、取引回数の上限値とは、電子権利格納装置200への格納回数の上限值となる。なお、実施の形態によっては、電子権利の発行、譲渡、消費の各トランザクション毎に、取引制限を別々に設ける等、多様な条件を指定することも可能である。

【0093】権利情報は、電子権利毎の固有情報が定義される。例えば、発行機関の識別子、権利の内容、発行者の署名等が定義される。

【0094】次に、これらの装置を用いて行う電子権利の取引（発行処理）について詳細に説明する。

【0095】（1）発行装置100は、電子権利生成部101により、有効期限（D）、サービスID（SID）、回数制限、権利内容を含む電子権利を生成する。また、検証装置104は乱数Cを生成する。

【0096】(2) 発行装置 100 は、上記 (1) によって生成された D, S I D, C を含む電子権利格納要求を電子権利格納装置 200 に送信する。なお、電子権利格納要求の送信では、電子権利自体 (所有権) はまだ移動していない。電子権利の移動については本発明では詳細に記載しないが、例えば特願 2000-038875 号等に記載されている権利情報固有の原本情報等の移動で実現される。

【0097】(3) 電子権利格納装置 200 は、格納制御部 202 により、履歴記録要求 Record (D, S I D, C) を生成し、履歴蓄積装置 205 に送る。

【0098】(4) 電子権利格納装置 200 は、履歴蓄積装置 205 により履歴データをその履歴蓄積部に記録し、結果を格納制御部 202 に送信する。

【0099】(5) 電子権利格納装置 200 は、格納制御部 202 により上記 (4) の結果を発行装置 100 に送る。

【0100】(6) 発行装置 100 は、検証装置 104 により上記 (4) の結果を検証する。詳細は実施の形態 1 と同じである。

【0101】(7) 発行装置 100 は、さらに累積回数 N がその電子権利に指定された回数制限以下であることを検証する。

【0102】(8) 発行装置 100 は、上記 (6), (7) の検証に成功した場合には、その電子権利を電子権利格納装置 200 に移動する。

【0103】(9) 電子権利格納装置 200 は、格納制御部 202 により受理した電子権利を電子権利格納部 204 に格納する。

【0104】電子権利格納装置に対する電子権利の格納は、発行だけではなく、別の電子権利格納装置からの譲渡によっても行われる。そこで、第一の電子権利格納装置 (以下、符号 200A で表す。) から第二の電子権利格納装置 (以下、符号 200B で表す。) に対して電子権利を譲渡する場合の流れについて以下に示す。

【0105】(1) 第一の電子権利格納装置 200A は、行使制御部 203 により、譲渡対象の電子権利の有効期限 D、サービス I D (S I D) を電子権利格納部 204 から取得する。また、検証装置 206 は乱数 C を生成する。

【0106】(2) 第一の電子権利格納装置 200A は、D, S I D, C を含む電子権利格納要求を第二の電子権利格納装置 200B に送信する。

【0107】(3) 第二の電子権利格納装置 200B は、格納制御部 202 により履歴記録要求 Record (D, S I D, C) を生成し、履歴蓄積装置 205 に送る。

【0108】(4) 第二の電子権利格納装置 200B は、履歴蓄積装置 205 により履歴データをその履歴蓄積部に記録し、結果を格納制御部 202 に送信する。

【0109】(5) 第二の電子権利格納装置 200B は、格納制御部 202 により上記 (4) の結果を第一の電子権利格納装置 200A に送る。

【0110】(6) 第一の電子権利格納装置 200A は、検証装置 206 により上記 (4) の結果を検証する。詳細は実施の形態 1 と同じである。

【0111】(7) 第一の電子権利格納装置 200A は、さらに累積回数 N がその電子権利に指定された回数制限以下であることを検証する。

【0112】(8) 第一の電子権利格納装置 200A は、上記 (6), (7) の検証に成功した場合には、その電子権利を第二の電子権利格納装置 200B に移動する。

【0113】(9) 第二の電子権利格納装置 200B は、格納制御部 202 により受理した電子権利を電子権利格納部 204 に格納する。

【0114】以上のステップにより、電子権利格納装置に電子権利が格納される前に、過去の取引履歴、上記実施の形態では電子権利の S I D 毎の格納履歴がチェックされるため、同一 S I D を持つ電子権利が制限回数以上格納されることを防止することができる。しかも、発行時だけではなく譲渡時もチェックすることが可能になる。

【0115】なお、個別の電子権利毎に異なる S I D を付与した場合には、二重使用を防止する方法の一つとしても利用可能である。

【0116】次に、本発明のその他のパリエーションについて述べる。

【0117】(1) 上記実施の形態では、履歴蓄積装置は、I C カード等の耐タンパ装置に実現されることを前提としているが、これをネットワーク装置上のサーバに記録することとし、累積取引回数が制限値を超えていないかのチェックをサーバに問い合わせることで、電子財布への格納を制御することもできる。このような方法は、従来の二重使用チェックサーバと類似しているが、本発明では、単純な二重使用チェックサーバと異なり、個別の電子権利単位の二重使用だけではなく、S I D による異なる単位で取引回数を制限できる等、柔軟なチェック機能を提供できる点が従来の方法と異なる。

【0118】(2) 上記実施の形態では、一つの電子権利に対して一つの S I D を付与しているが、複数の S I D を付与して、いくつかの制約条件を AND や OR で与えることも可能である。

【0119】(3) 上記実施の形態では、累積回数 N をサービス提供回数としているが、累積回数 N をサービス提供度数として管理し、一回のサービス提供に対して複数の度数を加算することによって、例えば一ヶ月当たりのローン限度額等の制御に適用することも可能である。

【0120】(4) 上記実施の形態では、履歴蓄積装置に履歴記録要求を送信した場合に累積回数 N が返される

が、Nを返す代わりに、回数制限値を超えたかどうかの真偽値を返すように実施しても良い。但し、この場合には、履歴蓄積装置内にS I D毎の回数制限値を記録しておき、累積取引回数が回数制限値を超えたかどうかを判定できるようにする必要がある。

【0121】(5) 上記実施の形態では、履歴データが格納される履歴蓄積部をI Cカード等の耐タンパ装置内に記録することを前提としているが、これをハードディスク等の通常の記憶媒体に格納し、履歴データのハッシュ値のみを耐タンパ装置に入れることで、履歴データの改ざんを防止しても良い。この場合、履歴データを追加、消去する度にハッシュ値を再計算する必要があるが、耐タンパ装置の記憶容量をさらに削減することができる。

【0122】

【発明の効果】以上述べたように、本発明によれば、利用者に提供するサービスで回数制限が設けられているものを、回数制限を超えて不正に利用したかどうかを、過去に受けたかどうかを含めて検証することができる。しかも、I Cカード等の耐タンパ装置に履歴が蓄積されるので、オフラインであっても安全に検証することができる。また、オフラインで検証できることは、通信コストが削減できるだけでなく、使用履歴を管理するためのセンタデータベースの開発コストや運用コストも削減できるという効果もある。

【0123】本発明の応用例としては、試供品の交換回数、レストランの試食回数、投票における投票回数、バーゲン品の購入回数、ゲームの出場回数、福利厚生施設の利用回数、コンサートチケットの購入回数、株主優待券の利用回数、免許証の違反回数、ローンの融資限度額等、多岐に渡る。従って、これらの制約条件は応用によって多種多様であるが、サービス提供者が勝手にS I Dと有効期限をセットして履歴を格納しても差し支えないので、一枚のI Cカードを多数のサービス提供者で共用することができる。また、これによりサービス提供者当たりのカードのコストを削減できるという効果がある。

【0124】履歴消去日時の実現に増加しかできないカウンタを用いることで、有効期限が切れたサービスに関する履歴を安全に削除することが可能になり、記憶領域が小さなI Cカードで実現しても実用的である。また、タイマ自体は耐タンパ装置の外に置いても安全であるから低コストで実現できるという効果がある。

【0125】従来、会員へのサービスの提供のため、紙

のクーポン券を郵送あるいは電子チケットをインターネットで配布していたのは、サービスの提供回数を限定するという目的があった。しかし、本発明の履歴蓄積機能を備える会員カードを持つ全ての会員に対してサービスを提供する場合には、カード内にサービス提供の履歴を検査することにより、サービスの提供回数を限定できるので、クーポン券等の発行が不要になるという利点がある。これは、クーポン券等を発行するためのシステムの開発コストや運用コストを削減できるという効果がある。

【図面の簡単な説明】

【図1】本発明の履歴蓄積装置の実施の形態の一例を示す構成図

【図2】履歴蓄積部に記録される履歴データの一例を示す説明図

【図3】履歴蓄積装置が履歴記録要求を受信した際の処理フローチャート

【図4】履歴蓄積装置が履歴消去要求を受信した際の処理フローチャート

【図5】本発明の検証装置の実施の形態の一例を示す構成図

【図6】検証装置が履歴蓄積装置に対して検証を行う際の処理フローチャート

【図7】検証装置が履歴蓄積装置に対して履歴消去を行う際の処理フローチャート

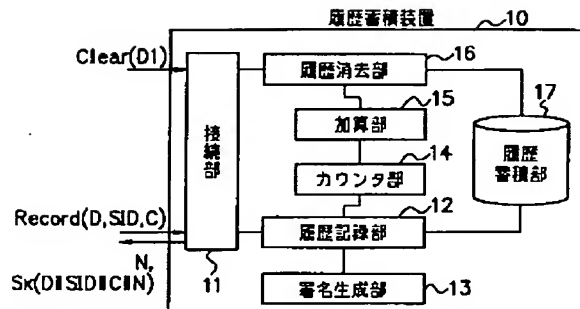
【図8】本発明の履歴蓄積装置と検証装置を利用した電子権利流通システムの実施の形態の一例を示す構成図

【図9】電子権利のデータ構造の一例を示す説明図

【符号の説明】

10：履歴蓄積装置、11：接続部、12：履歴記録部、13：署名生成部、14：カウンタ部、15：加算部、16：履歴消去部、17：履歴蓄積部、20：検証装置、21：乱数生成部、22：サービスI D記録部、23：有効期限記録部、24：検証制御部、25：署名検証部、26：履歴消去制御部、27：タイマ部、28：接続部、29：表示部、100：発行装置、101：電子権利生成部、102：電子権利発行部、103：通信部、104：検証装置、200：電子権利格納装置、201：通信部、202：格納制御部、203：行使制御部、204：電子権利格納部、205：履歴蓄積装置、206：検証装置、300：改札装置、301：電子権利改札部、302：通信部、304：検証装置、400：ネットワーク装置。

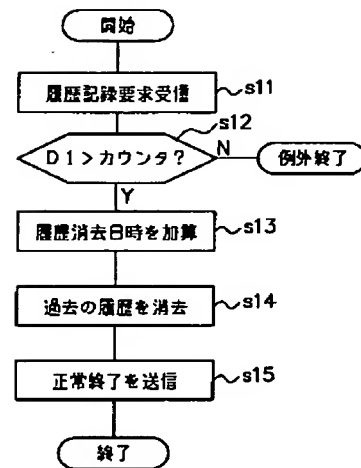
【図 1】



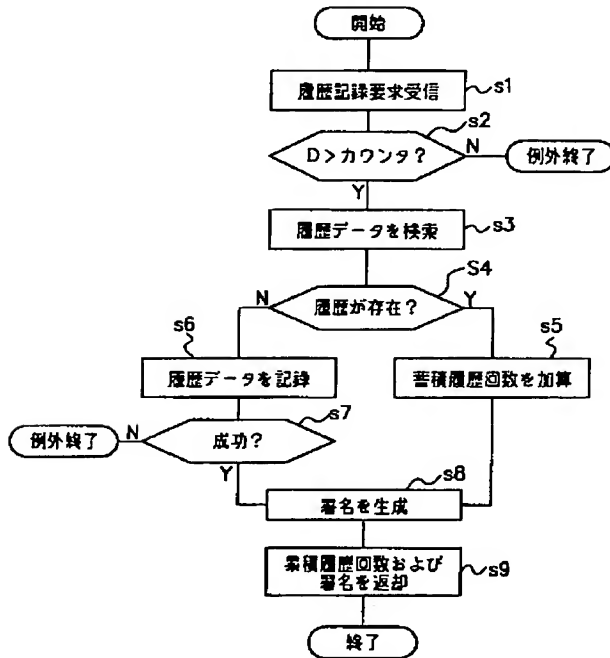
【図 2】

	有効期限 (D)	サービスID (SID)	累積回数 (N)
消去可能履歴	19991224	Bs3p42zK	2
カウンタ値	20000219	72J4VmNz	1
	20000616	Dk9R2?cA	12
消去不可履歴	20001003	0Yfk39wp	3
	20010101	3JxU82Ne	1

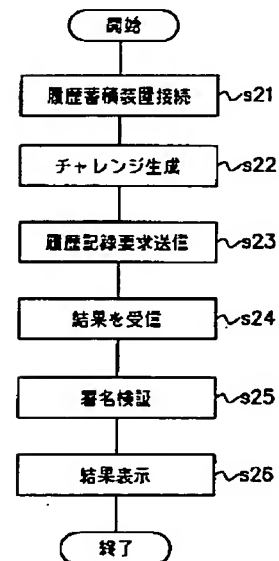
【図 4】



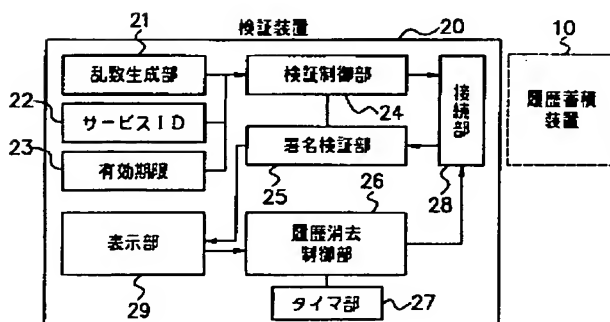
【図 3】



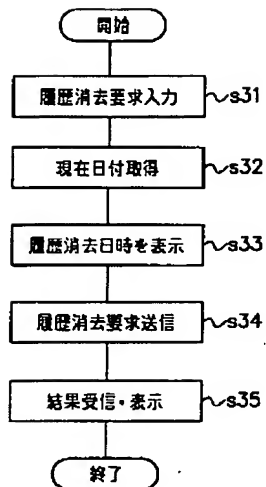
【図 6】



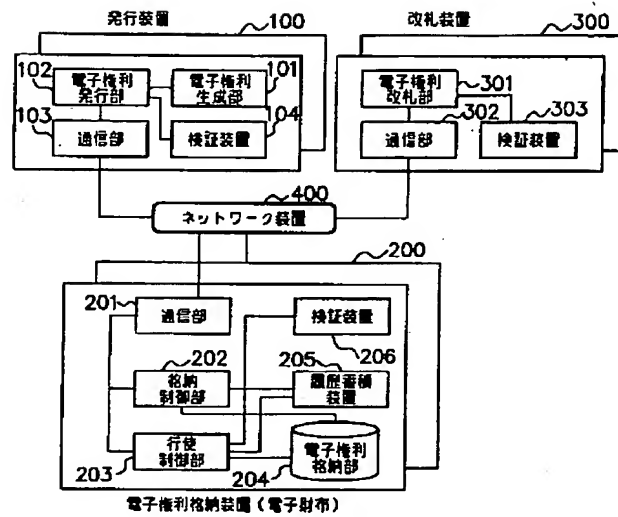
【図 5】



【図 7】



【図 8】



【図 9】

権利ID	有効期限	回数制限	権利情報
Bs3p42zK	19991224	4	http://ticket.ntt.co.jp/a-restrant/a-coupon/001234
Dk9R21cA	20000616	20	http://ticket.ntt.co.jp/a-shop/a-gift/002222
3JxU82Ne	20010101	1	http://ticket.ntt.co.jp/a-facility/a-pass/009999

フロントページの続き

(72)発明者 西原 琢夫
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

Fターム(参考) 5B049 AA05 BB00 CC13 CC31 EE02
EE22 FF08
5B055 EE02 KK05 KK15
5D110 AA13 DA11 DA13 DA17 DB09
DC05 DC06 DD13 DD16 DE04

THIS PAGE BLANK (USPTO)